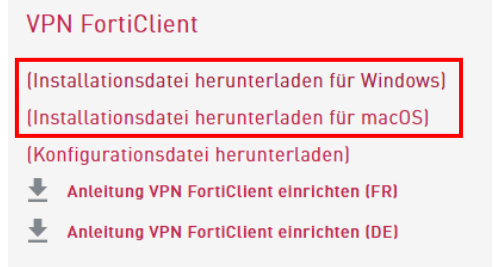
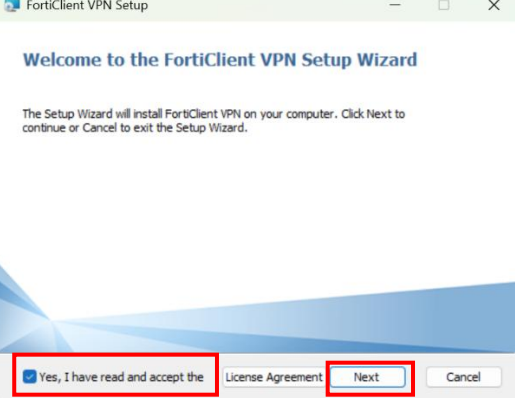
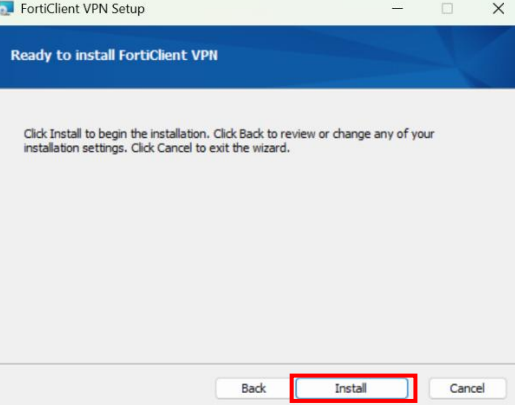
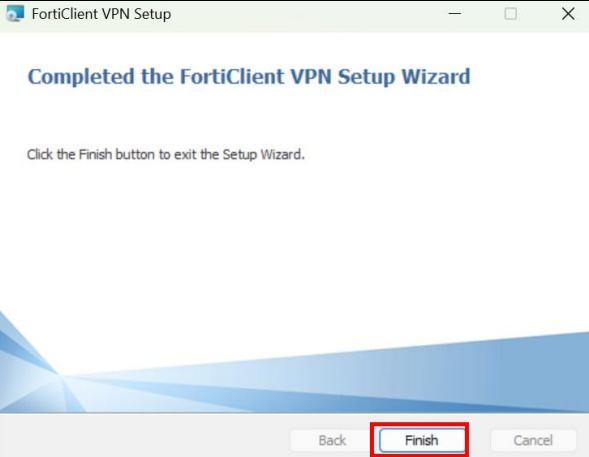


Table des matières

1.	Installation de FortiClient	2
1.1.	Instructions	2
2.	Configuration automatique	3
2.1.	Droits d'administrateur	3
2.2.	Instructions	3
3.	Configuration manuelle	5
3.1.	Cas d'utilisation	5
3.2.	Instructions	5

1. Installation de FortiClient

1.1. Guide

Télécharger le fichier d'installation de FortiClient (fichier d'installation macOS)	
Lancer le fichier d'installation	
Cliquer sur « Yes, I have read... » Cliquer sur « Next »	
Cliquez sur « Install »	
Cliquez sur « Finish ». FortiClient est ainsi installé. Pour la configuration, passez au chapitre 2 ou 3	

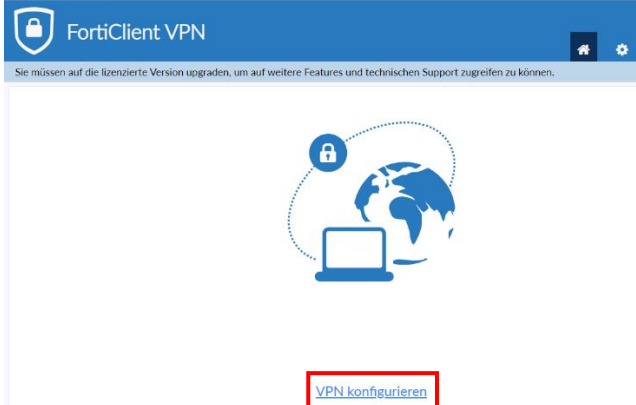
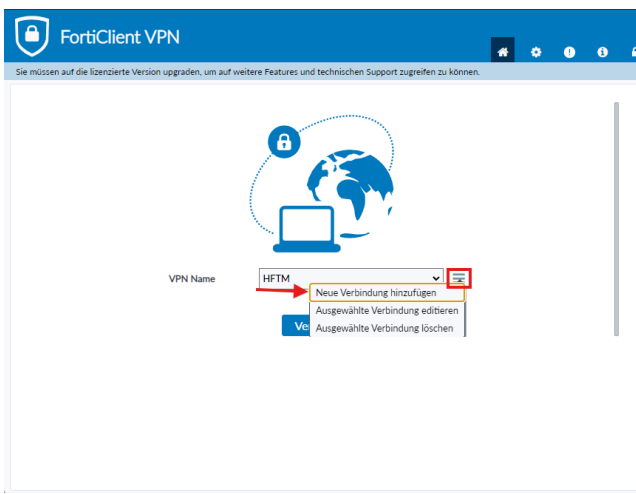
2. Configuration automatique

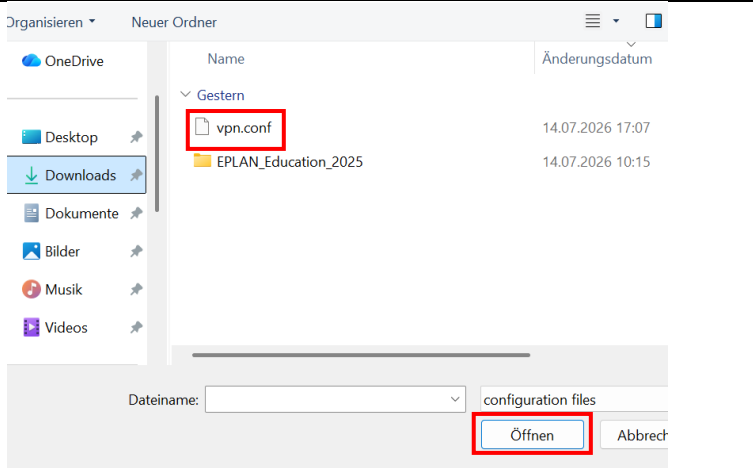
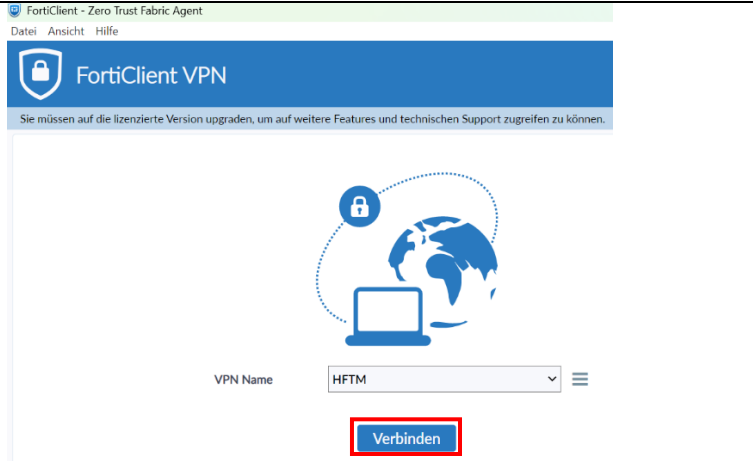
2.1. Droits d'administrateur

La configuration automatique **ne** peut être effectuée **que** si l'appareil dispose de **droits d'administrateur**.

Cette méthode supprime également **toutes les connexions VPN FortiClient configurées jusqu'à présent**.

2.2. Instructions

Télécharger le fichier de configuration FortiClient	VPN FortiClient (Installationsdatei herunterladen für Windows) (Installationsdatei herunterladen für macOS) (Konfigurationsdatei herunterladen) ↓ Anleitung VPN FortiClient einrichten (FR) ↓ Anleitung VPN FortiClient einrichten (DE)
Ouvrir FortiClient Cliquer sur « Configurer le VPN » Ou, si une connexion est déjà établie, cliquer sur « Ajouter une nouvelle connexion »	FortiClient - Zero Trust Fabric Agent Datei Ansicht Hilfe FortiClient VPN Sie müssen auf die lizenzierte Version upgraden, um auf weitere Features und technischen Support zugreifen zu können.  FortiClient VPN Sie müssen auf die lizenzierte Version upgraden, um auf weitere Features und technischen Support zugreifen zu können. 

Sélectionner « XML » Sélectionnez ensuite « Importer la configuration XML ».	
Rechercher et ouvrir le fichier « vpn.conf »	
Saisissez le mot de passe suivant : hftm*1234	
Une fois l'importation terminée, des droits d'administrateur sont nécessaires pour valider la configuration.	
Une fois la confirmation effectuée, la connexion « HFTM » s'affiche. Cliquez ensuite sur « Se connecter »	

--	--

Configuration manuelle

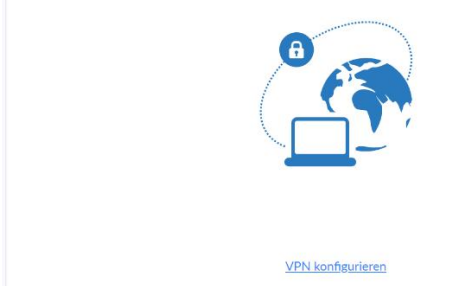
2.3. Cas d'utilisation

La configuration manuelle est effectuée si des connexions existantes **doivent être conservées** ou en cas **d'absence de droits d'administrateur**

2.4. Instructions

Cliquez sur « Configurer le VPN »

Ou, si une connexion existe déjà, cliquez sur « Ajouter une nouvelle connexion »



The screenshot shows the FortiClient VPN application window. At the top, there's a blue header with the FortiClient logo and 'FortiClient VPN'. Below the header, there's a message: 'Sie müssen auf die lizenzierte Version upgraden, um auf weitere Features und technischen Support zugreifen zu können.' In the center, there's a graphic of a globe with a laptop and a lock icon. At the bottom, there's a button labeled 'VPN konfigurieren'.

Régler le VPN sur « VPN IPsec »



The screenshot shows the FortiClient VPN application window with the 'Neue VPN Verbindung' dialog box open. The dialog has a title bar 'Neue VPN Verbindung' and a 'VPN' label. There are two buttons: 'SSL-VPN' and 'IPsec VPN'. The 'IPsec VPN' button is highlighted with a red box. Below the buttons, there's a red rectangle.

Effectuez les réglages de base suivants : - Nom de la connexion : HFTM - Passerelle distante : vc.hftm.ch - Méthode d'authentification : Clé - Saisir la clé suivante : XYGMwZpm%SYXC1rR4z - Paramètres d'authentification unique : Activer - Personnaliser le port : 9443	Neue VPN Verbindung VPN: SSL-VPN IPsec-VPN XML Verbindungsname: HFTM Beschreibung: Verbindung zur hftm Remote Gateway: vc.hftm.ch Authentifizierungsmethode: Schlüssel Failover SSL VPN: [Keines] Single Sign On Settings: ☒ Aktiviere Single Sign On (SSO) für den VPN Tunnel Port anpassen: 9443 ☐ Verwende externen Browser als User-Agent für SAML
Ouvrir les paramètres avancés Paramètres VPN : - IKE : version 2	Experteneinstellungen VPN Einstellungen IKE: ☐ Version 1 ☒ Version 2 Address Assignment: ☒ Modus Konfiguration ☐ Manuell setzen ☐ DHCP über IPsec Encapsulation: ☒ IKE UDP Port ☐ IPsec over TCP ☐ Auto (UDP fallback TCP) 500
Paramètres de la phase 1 : - Proposition IKE : comme sur l'image - Groupe DH : 20, 21	Phase 1 IKE Vorschlag: Verschlüsselung AES128 Authentifizierung SHA256 Verschlüsselung AES256 Authentifizierung SHA256 DH Gruppe: ☐ 1 ☐ 2 ☐ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☒ 20 ☒ 21 Schlüssel: 86400 Sek Gültigkeitsdauer: Optional Lokale ID: ☐ Dead Peer Erkennung ☒ NAT Traversal ☐ Aktiviere Local LAN
Paramètres de la phase 2 : - Proposition IKE : comme sur l'image - Groupe DH : 21	Phase 2 IKE Vorschlag: Verschlüsselung AES128 Authentifizierung SHA256 Verschlüsselung AES256 Authentifizierung SHA256 Schlüssel: ☒ 43200 Sekunden ☐ 5120 KBytes Gültigkeitsdauer: ☒ Replay Erkennung aktivieren ☒ Perfect Forward Secrecy (PFS) aktivieren DH Gruppe: 21
Pour finir, cliquez sur « Enregistrer »	Abbrechen Sichern

Cliquez ensuite sur « Se connecter » et connectez-vous avec vos identifiants Office.

La connexion au réseau hftm s'établit alors.

